

ABSTRACT

The packet rate limiting method and system is used for detecting and blocking the effects of DoS attacks on IP networks. The method uses an ACL counter that stores an action parameter in the first 3 most significant bits and uses 13 bits as a packet counter. A rate limit is enforced by setting the packet counter to an initial value, and resetting this value at given intervals of time. The action parameter enables the ACL to accept or deny packets based on this rate limit. If the number of packets in the incoming flow saturates the packet counter before the reset time, the packets are denied access to the network until the counter is next reset. The denied packets may be just discarded or may be extracted for further examination.